CIBERCRIMINALIDAD Y PERSPECTIVA VICTIMOLÓGICA: UN ENFOQUE GENERAL EXPLICATIVO DE LA CIBERVICTIMIZACIÓN

JOSÉ R. AGUSTINA*

Fecha de recepción: 21/05/2014
Fecha de aprobación: 25/11/2014

RESUMEN: En el presente artículo se describe, con un propósito orientado a la prevención del ciberdelito, el modo en que el comportamiento de la víctima en el ciberespacio influye decisivamente en la génesis del delito, señalándose al mismo tiempo algunos factores ambientales que empujan a las víctimas a adoptar elevados riesgos de victimización. Para ello, se esbozan, en primer lugar, los motivos que explican por qué el diseño de las arquitecturas digitales incrementan notablemente las oportunidades delictivas (que facilitan la cibervictimización) y cómo las notas definitorias del ciberespacio afectan sensiblemente en las actividades cotidianas de las personas y, más aún, en la inclinación del ser humano a adoptar estilos de vida de mayor riesgo. Seguidamente, se muestran cómo las perspectivas victimológica y victimodogmática revisten una singular importancia no solo en la explicación del evento delictivo y en las estrategias de prevención sino también en la atribución de responsabilidad jurídico-penal.

Partiendo de las características criminógenas de las arquitecturas digitales, se identifica un conjunto de rasgos (psicológicos, antropológicos y sociológicos) que inciden en el perfil de las víctimas o, cuando menos, de determinados grupos de víctimas. Dicho análisis estará enfocado a des-

* Universitat Internacional de Catalunya. Barcelona, España. El presente artículo ha sido realizado en el marco del Proyecto de Investigación financiado por el Ministerio de Ciencia e Innovación, DER2011-26054, titulado "Cibercriminalidad: detección de déficits en su prevención jurídica y determinación de los riesgos de victimización para una mejor prevención situacional criminológica".

cribir cómo el entorno influye en el modo de pensar y actuar de las personas, dando lugar con posterioridad a analizar ciertas consideraciones sobre la calidad y relevancia del consentimiento, sus déficits y la forma de afrontarlos. Finalmente, se analizan de forma sintética algunas particularidades de las estrategias de prevención de la ciberdelincuencia (o mejor, de la cibervictimización), y se apuntan algunas reflexiones críticas sobre ciertos estereotipos en relación con el perfil del ofensor y de la víctima.

PALABRAS CLAVE: cibervictimización, prevención del ciberdelito, efecto desinhibidor, teoría de las actividades rutinarias y TIC.

ABSTRACT: We live immersed in a society that has undergone vertiginous changes in a remarkably short amount of time. Researchers in the fields of sociology, psychology, behavioural sciences, and law are trying to comprehend the more-or-less radical rise of a new relational paradigm of personal and social interactions. The proliferation of ICT is a reality that continues to advance inexorably, permeating everything in our daily lives. We often hear about an intergenerational 'digital gap'; however, aside from the fact that this supposed gap will soon cease to exist, technology actually affects everyone. Crime dynamics and, consequently, victimisation are not alien to the set of changes wrought by the digital era.

With a focus on the prevention of cybercrime, in the following lines I will describe the way in which the behaviour of victims in cyberspace decisively elevates their risk of victimisation, singling out some environmental predictors of online victimisation. To do so, I will first outline why the design of digital architectures notably increases criminal opportunities and facilitates cyber-victimisation, and how the defining traits of cyberspace affect people's daily lives and incline them to adopt riskier lifestyles. Then, I will try to show the importance of the victimological perspective in explaining the criminal event, designing prevention strategies and assigning criminal liability. The analytical perspective is supported, principally, by routine activity theory (Cohen and Felson 1979) and lifestyle theory (Hindelang, Gottfredson and Garofalo 1978), along with the interesting work of Suler (2004). Based on the latter, I will describe a set of psychological, anthropological, and sociological traits that comprise the profile of victims or, at least, certain groups of victims. This analysis will focus on describing how the surroundings influence one's thoughts, desires, and actions. Finally, I will summarise some cybercrime prevention strategies based on Miró's contribution (Miró 2012).

KEYWORDS cybervictimization, cybercrime prevention, disinhibition effect, routine activities approach and ICT.

SUMARIO: I. Introducción: arquitecturas digitales y naturaleza humana; tecnología y delito. II. La irrupción de la perspectiva victimológica en un análisis global del delito. III. Algunas consideraciones victimológicas aplicadas al ciberespacio. IV. Lugar y delito: arquitecturas digitales, convergencia de espacios y divergencia esquizofrénica. V. Entornos victimo-genésicos y perfiles victimológicos: el efecto de desinhibición en el comportamiento *online* y la ingenuidad/irreflexibilidad de las víctimas. A) *Online disinhibition effect*. B) Víctimas ingenuas e irreflexivas. VI. Estrategias de prevención y autoprotección de la víctima en el ciberespacio. VII. Algunas paradojas: perfil de los ofensores *versus* víctimas no tan ingenuas. VIII. Reflexiones finales.

I. INTRODUCCIÓN: ARQUITECTURAS DIGITALES Y NATURALEZA HUMANA; TECNOLOGÍA Y DELITO

Vivimos en la actualidad inmersos en una sociedad que ha experimentado cambios vertiginosos en un lapso de tiempo significativamente breve. Desde la Sociología, la Psicología y las ciencias del comportamiento humano, la Política o el Derecho, entre otras disciplinas, se viene tratando de asimilar y comprender la novedad, más o menos radical, de un nuevo *paradigma relacional* en las interacciones personales y sociales. La proliferación y generalización en el uso de las Tecnologías de la Información y Comunicación es ya una realidad que, inexorablemente, sigue avanzando, inmiscuyéndose en nuestra vida cotidiana, permeándolo todo. Con frecuencia se hace mención a una "brecha digital" intergeneracional; sin embargo, además de que dicha brecha en breve dejará de existir, la tecnología afecta de hecho a toda la población. Y a todo este conjunto de cambios derivados de la era digital no es ajeno el ámbito de la delincuencia y, por consiguiente, de la victimización.

En las líneas que siguen trataré de describir, con una finalidad centrada en la prevención del ciberdelito, el modo en que el comportamiento de la víctima en el ciberespacio incide decisivamente en el elevado riesgo de victimización, tratando de señalar algunos factores ambientales predictores de la victimización *online*[1]. Para ello, esbozaré, en primer lugar, los motivos que explican por qué el diseño de las arquitecturas digitales

[1] El presente artículo es una versión ampliada y mejorada de un texto anterior del autor publicado con el título "Victimización en el ciberespacio. Victimología y victimodogmática en el uso de las TIC. Desfragmentación del yo en la era digital: 'disinhibition effect', esquizofrenia digital e ingenuidad en el ciberespacio" en la importante obra coordinada por J.M. Tamarit y N. Pereda "Las respuestas de la Victimología ante las nuevas formas de victimización" (2014), BdeF-Edisofer.

incrementan notablemente las oportunidades delictivas que facilitan la cibervictimización y cómo las notas definitorias del ciberespacio afectan sensiblemente en las actividades cotidianas de las personas y, más aún, en la inclinación del ser humano a adoptar estilos de vida de mayor riesgo. Seguidamente, trataré de mostrar que la perspectiva victimológica reviste una singular importancia no solo en la explicación del evento delictivo sino en las estrategias de prevención y en la atribución de responsabilidad jurídico-penal. La perspectiva de análisis desde la que abordaré tanto dichas cuestiones como las restantes se apoya, de modo principal, en la *teoría de las actividades cotidianas*[2] y en la *teoría de los estilos de vida*[3], así como en el conjunto de enfoques criminológicos englobados en las *teorías de la oportunidad*. Ciertamente muy cercana a las *teorías de la oportunidad* se halla la teoría formulada por Jaishankar[4], en la que trata de mostrar por qué las personas se comportan de modo diferente cuando se trasladan del espacio físico a al espacio virtual. Factores criminógenos fundamentales presentes en el ciberespacio, a su juicio, son la falta de disuasión asociada a la anonimidad, así como la propensión delictiva de algunas personas que se sienten reprimidas en el mundo *real* a liberarse *online* y cometer delitos en el ciberespacio.

A continuación, me centraré, partiendo de las características criminógenas de las arquitecturas digitales, en la descripción del conjunto de rasgos (psicológicos, antropológicos y sociológicos) que definen el perfil de las víctimas o, cuando menos, de determinados grupos de víctimas. Dicho análisis estará enfocado a describir cómo el entorno influye en el modo de pensar, querer y actuar de las personas. Finalmente, me referiré de forma sintética a las estrategias de prevención de la ciberdelincuencia (o mejor, de la cibervictimización), concluyendo mis reflexiones con una revisión crítica de ciertos estereotipos en relación con el perfil del ofensor y de la víctima.

Ante el avance de nuevas formas de delincuencia que se asocian al creciente aumento de usuarios en Internet, ya sostuve en otro lugar[5] que la Criminología debería acometer con determinación el estudio de los factores criminógenos que facilitan la comisión de actos ilícitos. Las ar-

[2] Cohen, L.E. y Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* 44: 588-608.

[3] Hindelang, M., Gottfredson, M. y Garofalo, J. (1978).*Victims of Personal Crime: an Empirical Foundation for a Theory of Personal Victimization*. Cambridge MA: Ballinger.

[4] Jaishankar, K. (2008). Space transition theory of cybercrimes.In F. Schmalleger& M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283−301).Upper Saddle River, NJ: Prentice Hall.

[5] Agustina, J.R. (2009). Arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual. *International E-Journal of Criminal Sciences*, núm. 3 (2009).

quitecturas digitales generan una atmósfera de anonimato que protege, promueve y alimenta nuevos modos de atentar contra las personas e instituciones. Además, por la propia constitución de la red y las posibilidades de intercomunicación que suponen las TIC, las conductas delictivas adquieren una potencialidad lesiva que viene a multiplicar los posibles daños a terceros. En este sentido, resulta necesario profundizar y determinar las relaciones existentes entre (i) el modo de configurar los límites y las reglas que se aplican en ese espacio virtual y (ii) la consecuente atracción o generación de delincuencia que comporta. Sin embargo, las estrategias de prevención situacional topan con los límites derivados de la privacidad de los usuarios de Internet, la libertad de expresión y la libertad de navegación.

Ciertamente, el ciberespacio sigue siendo en la actualidad un *lugar oscuro* que fomenta el anonimato. Sin embargo, en la medida en que la preocupación por el ciberdelito va en aumento, cobra mayor fuerza la idea de que ciertos cambios estructurales en las arquitecturas digitales podrían suponer un giro repentino «del mismo modo a como sucedió con la irrupción de la luz de gas y la electricidad» en las oscuras calles de las ciudades en las que se propiciaba la comisión de delitos. Por tanto, desde esa perspectiva, deberían buscarse modos de arrojar luz sobre los usuarios en el ciberespacio[6].

No obstante, la adopción de mecanismos de transparencia y control en la navegación por Internet, atentaría contra la mencionada libertad de navegación, en la medida en que el establecimiento de un *principio de privacidad limitada* conllevaría una menor libertad de actuar sin ser identificado. En esta discusión, la tensión entre libertad (privacidad) *versus* seguridad (prevención) ha centrado el debate social y político. Así, el dilema es claro: se debe optar entre una mayor libertad de navegar por la red, libre de controles, sin necesidad de identificación alguna, y una mayor tolerancia respecto al aprovechamiento que algunos obtienen de las nuevas oportunidades delictivas, con naturales a un espacio donde el anonimato tiene claros efectos criminógenos[7]. En este sentido,

---

[6] Katyal, N.K. (2003). Digital Architecture as Crime Control, 111 *Yale Law Journal* 1039.

[7] En la fase final de revisión del presente texto ha saltado a la opinión pública el escándalo de la vigilancia secreta de las comunicaciones en el ciberespacio por parte del gobierno norteamericano, a raíz de la filtración de Edward Snowden, un trabajador subcontratado de la CIA para servicios de espionaje informático ("Un joven experto en espionaje pone contra las cuerdas a Obama", *El País*, 10 de junio de 2013). Para un interesante análisis sociológico de las tensiones actuales de la privacidad frente a necesidades

la red es –dentro de la tipología de lugares acuñada por Brantingham y Brantingham[8]– tanto un lugar criminógeno, en el sentido de que por sus mismas condiciones genera delincuencia (*crime-generator*), como un espacio propicio que atrae al delincuente a cometer sus delitos (*crime-attractor*), en el que existen menores riesgos de ser detectado y abundan distintos objetivos altamente atractivos.

Sin embargo, no parece que las sociedades actuales vayan a decantarse por la opción de convertir Internet en un lugar seguro a ultranza, en el que las personas se desenvuelvan *con luz y taquígrafos*, a pesar de que existan propuestas en favor de una mayor seguridad y se pretendan introducir ciertas mejoras. Por ese motivo, cobra una mayor importancia centrarse en cómo proteger a las víctimas potenciales frente a los riesgos que caracterizan los entornos virtuales y ahondar en las causas que llevan a las personas a un uso imprudente de las TIC y de Internet. La cuestión estriba, entonces, en analizar la vulnerabilidad de las víctimas y corregir los déficits en la utilización de las TIC, corrigiendo su natural inclinación a no tomar en consideración los riesgos derivados de su propia conducta.

De este modo, debemos plantearnos qué resortes de la naturaleza humana se ven influidos por las arquitecturas digitales. A este respecto, Marcus Felson propuso desde una perspectiva general estudiar detenidamente la naturaleza humana para comprender el comportamiento delictivo, examinando cómo varían las situaciones humanas (en función del contexto) y el modo en que éstas influyen en nuestra comprensión del delito. Sus reflexiones son aplicables tanto a la explicación de la inclinación al delito por parte del ofensor, como a la inclinación de las víctimas a adoptar comportamientos sin las necesarias cautelas.

> «En primer lugar, consideremos la visión del hombre desde el punto de vista de su fragilidad humana básica. No es más que la concepción bíblica relativa a que los seres humanos son moralmente débiles y requieren todos y cada uno de ellos ayuda de la sociedad para resistir a las tentaciones y presiones que reciben. Así, las personas con creencias morales tienen dificultades en la práctica para adecuarse a sus propias referencias, siendo capaces de hacer el bien y el mal. El problema práctico reside en cómo ayudar a las personas a superar sus debilidades a través de una determinada estructura social que reduzca las tentaciones. Ciertamente, algunas personas

de carácter público (por ej. en caso de ex delincuentes sexuales, terrorismo o historiales médicos), véase la interesante obra de Amitai Etzioni (2012).

[8] Brantingham P. y Brantingham P. (1995). Criminality of place: Crime generators and crime attractors. *European Journal on Criminal Policy and Research* 3(3): 5–26.

> son más "frágiles" que otras, pero todas poseen algún grado de fragilidad y vulnerabilidad. Esta afirmación resulta bastante diferente a decir que las personas no poseen creencias lo bastante firmes sobre lo que está bien y está mal. Por el contrario, se refiere a que las personas tienen dificultades para poner en práctica sus creencias morales, es decir, para resistir frente a la tentación»[9]

¿Y cómo se aprovecha el ofensor de las fragilidades de la víctima? Desde antiguo se resaltaron dos formas tradicionales por las que se podía cometer un delito: *duobus modis fit iniuria: aut vi, aut fraude*. Como muestra esta conocida máxima, extraída de la obra de Marco Tulio Cicerón[10], se venía considerando que, en realidad, todo delito –y, por tanto, toda victimización– puede reducirse a una única disyuntiva en su modalidad comisiva. Así, el daño infligido a toda víctima de un delito puede cometerse mediante fuerza o a través de engaño. Posteriormente, sin embargo, al catálogo de delitos clásicos se añadieron los delitos imprudentes, en los que no media, por definición, fuerza o engaño en el *modus operandi* del ofensor.

Por las propias particularidades de los contextos virtuales en los que tienen lugar las distintas formas de cibervictimización, el recurso al engaño constituye el modo comisivo por antonomasia, sin perjuicio de que también se cometan a través de las TIC, por ejemplo, delitos contra el honor (injurias y calumnias), en los que no se suelen emplear artificios engañosos. No obstante, incluso en tales casos los ofensores, con frecuencia, recurren a la simulación o al anonimato para lograr la impunidad de sus acciones.

En la propia naturaleza humana radica esa inclinación a la mentira como mecanismo de manipulación y de causar daño a terceros, especialmente si la víctima reúne ciertas características que la hacen más vulnerable o si el contexto propicia un mayor número de ocasiones idóneas, entre otras características, porque el ciberespacio fomenta actitudes de excesiva confianza, ingenuidad o irreflexión, aprovechadas por el ofensor para cubrirse de una apariencia de veracidad desde el anonimato.

En este sentido, el fraude o engaño es un arte antiguo, pero el ciberespacio proporciona un número mucho más elevado de víctimas, incluso para un solo ofensor. En efecto, los cambios tecnológicos conducen a importantes cambios en el modo de pensar y actuar de las personas, teniendo pues repercusiones significativas no sólo de naturaleza antropo-

---

[9] Felson, M. (1994).*Crime and Everyday Life* (1st ed.). Thousand Oaks, CA: Pine Forge Press.

[10] Cicerón, Marco Tulio *De officiis*, Liber I, Caput 13.

lógica, sociológica o cultural, sino en las tasas de delito[11]. Es decir, la tesis principal de Ogburn es que primero irrumpe un cambio tecnológico, al que le sucede después un cambio sociológico o cultural, derivándose de todo ello un cambio de tendencia en el número y *modus operandi* de los delitos. Marcus Felson[12] mantiene que la descripción sociológica que efectúa Ogburn sugiere una importante lección en el ámbito criminológico, cual es, que debemos dejar de asumir que los cambios en la delincuencia vendrán por los cambios introducidos en la cultura. Sin negar que ésta tenga relevancia, afirma en este sentido que la tecnología es, en última instancia, la principal fuerza conductora de las transformaciones sociales y, por tanto, los cambios tecnológicos son los que provocan alteraciones en las formas de delincuencia.

Las consecuencias de todo ello se manifiestan intensamente, como es lógico, a nivel antropológico. Parece, pues,que los cambios tecnológicos potencian a niveles superiores la ingenuidad y estupidez humana. Y así, con ayuda de las TIC *cada minuto nace un idiota nuevo* –conocida frase que se atribuye a Phineas T. Barnum: «there's a sucker born every minute»)–, e Internet los conecta entre sí y, sobre todo, con quienes pueden convertirlos en víctimas, y ello sin necesidad de interactuar en persona.

Con todo, actualmente todavía siguen siendo pocos y de escasa fiabilidad los estudios sobre el nivel de incidencia de las distintas formas de cibervictimización, aunque en los existentes se constata que el número de cibervíctimas se incrementa anualmente[13]. Los datos estadísticos son poco fiables por varias razones[14]. En primer lugar, la cifra negra es muy alta al tratarse de delitos que no pueden detectarse sin un nivel muy superior en investigación. La investigación policial en el ciberespacio es especialmente compleja debido, en ocasiones, a la alta sofisticación con que cuentan los ciberdelincuentes; y/o a que el delito se comete mediante sistemas o canales que dificultan la identificación del ofensor (correos electrónicos (re)enviados anónimamente, sistemas de encriptación de mensajes, utilización de terceras personas mediante suplantación de

[11] Ogburn, W.F. (1964). On Culture and Social Change: Selected Papers (Ed. Otis Dudley Duncan). Chicago: University of Chicago Press.

[12] Felson, M. (1997). Technology, Business and Crime. En Felson, M. y Clarke, R.V. (ed.), *Business and Crime Prevention*, Monsey, NT: Willow Tree Press, pp. 81–96.

[13] Gordon, M.P., Loef, M.P., Lucyshyn, W., y Richardson, R. (2004). *CSI/FBI computer crime and security survey*. Los Angeles: Computer Security Institute.

[14] Choi, K. (2008). Computer Crime, Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, vol. 2, enero-junio.

identidad, etc.)[15]. Además, pocos delitos cometidos en el ciberespacio se llegan a denunciar a las autoridades[16].

Conviene resaltar, no obstante, los resultados del primer estudio realizado en España sobre cibervictimización[17]. Dichos resultados muestran, en efecto –como apuntábamos–, una prevalencia de los ciberdelitos cuyo objetivo final es el ciberfraude. Concretamente, más del 45% de la población española reconoce haber recibido correos proponiéndoles algún tipo de favor o negocio económico sospechoso de ser engañoso; y un 43,6% manifiesta haber recibido algún correo cuya identidad del remitente era falsa. En cuanto a infecciones de *malware*, el 72,8% de la población reconoce haberlas sufrido. Y a todo ello hay que sumar el significativo dato de que un 24,4% de la población española reconoce haber sufrido efectivamente una pérdida patrimonial víctima de un ciberfraude.

II. LA IRRUPCIÓN DE LA PERSPECTIVA VICTIMOLÓGICA EN UN ANÁLISIS GLOBAL DEL DELITO

Ante el panorama que se acaba de presentar, en las líneas que siguen trataré de analizar cómo el papel que desempeña la conducta de la víctima en su propia cibervictimización debería llevarnos a plantear la necesidad de adoptar ciertas estrategias de prevención para reducir su exposición a riesgos innecesarios. La premisa fundamental de la que se debe partir es que el comportamiento de la víctima juega un papel decisivo en el acontecer delictivo. Ello es así no sólo en el espacio físico-corporal, sino también en el espacio virtual, si bien con algunas modulaciones y adaptaciones en función de las particularidades de uno y otro contexto.

---

[15] Furnell, S. (2002). *Cyber crime: Vandalizing the information society*. London: Addison Wesley.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.) *Crime and the Internet*. London: Routledge, 23-45.Yar, M. (2005). The novelty of 'cyber crime': An assessment in light of routine activity theory. *EuropeanSociety of Criminology*, 2, 407-427.

[16] Standler, B.R. (2002). *Computercrime*, en *http://www.rbs2.com/ccrime.htm* (última consulta el 31 de mayo de 2013).

[17] *Vid.* Miró, F. y García, N. (2012). "Encuesta Nacional de victimización en el ciberespacio", presentada en la conferencia La victimización en el ciberespacio, impartida en el IX Congreso Español de Criminología, Girona, 2012, estudio citado en Miró Llinares, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología*: 15-12 (2013). Véase, también, Miró, F. (2013). "La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio". Revista Española de Investigación Criminológica: REIC, Nº. 11, Artículo 5.

Sin embargo, antes de entrar a analizar la conducta de la víctima en espacios virtuales y sus implicaciones, me referiré de forma sintética a cómo irrumpió en el escenario criminológico y jurídico-penal dicha perspectiva y las implicaciones que se han seguido de este cambio de paradigma.

En efecto, tal y como ha puesto de manifiesto la investigación criminológica, se puede afirmar que el comportamiento de la víctima constituye un elemento esencial para explicar por qué una persona sufre *en sus carnes* un hecho delictivo. En ese sentido, el estudio del rol de la víctima en el acontecer delictivo resulta decisivo para identificar las adecuadas estrategias de prevención. A decir verdad, son las propias víctimas las que permiten de algún modo que sus ofensores tengan acceso a interaccionar con ellas. En ocasiones, dicho acceso será inevitable (piénsese, por ejemplo, en la necesidad de movimientos a través de espacios públicos); pero no siempre será inevitable o, al menos, algunos riesgos de victimización serán evitables si se adoptan las debidas cautelas. Ciertamente, todas las personas están en su derecho de *salir a la calle* para satisfacer sus necesidades sociales básicas; pero, a pesar de que ese derecho no decaiga nunca, si uno desea evitar ser víctima de un delito debería adoptar ciertas medidas de autoprotección, especialmente si pretende, por ejemplo, pasear solo a según qué horas de la noche por según qué barrios.

Por tanto, si se asume que la exposición voluntaria de la propia víctima ante potenciales ofensores permite y facilita su victimización, se puede concluir, aunque sea solo desde una perspectiva criminológica, que con su comportamiento deviene, de algún modo, co-causante de su propia victimización, en la medida en que estuvo en sus manos la posibilidad de evitar la interacción con su ofensor.

Como es lógico, debe distinguirse entre considerar a la víctima co-causante (perspectiva criminológica) y co-responsable (perspectiva jurídico-penal). La primera perspectiva se dirige básicamente a identificar estrategias de prevención: pretende, pues, *explicar para prevenir*, desde un punto de vista *ex ante*. La segunda, en cambio, lo único que pretende es asignar o distribuir responsabilidad penal entre el ofensor y la víctima, en caso de que ésta tuviera parte de culpa (jurídica), como veremos, en la producción del resultado delictivo: por tanto, se dirige a atribuir o disminuir la responsabilidad penal del ofensor en el ámbito jurisdiccional, desde un punto de vista *ex post facto*.

En líneas generales, históricamente se venía asumiendo que el posible comportamiento negligente de las víctimas no podía implicar responsabilizarles de ningún modo por el hecho padecido en su persona, ni disminuir un ápice el grado de la responsabilidad penal del ofensor. Sin

embargo, desde hace unas décadas lo que parecía una afirmación rotunda se ha visto profundamente revisado por la *perspectiva victimológica* y su traslación al ámbito de responsabilidad penal, lo que ha venido a denominarse *victimodogmática*[18]. Dicha perspectiva de análisis ha llevado a que, en ocasiones, la co-responsabilidad de la víctima, sobre todo en delitos imprudentes (aunque no sólo: por ejemplo, en el delito de estafa), conlleve una disminución de la responsabilidad del acusado porque, desde dichos postulados victimodogmáticos, se constató que hubo una concurrencia de culpas relevante entre acusado y víctima o una negligencia en los deberes de autoprotección de la víctima.

En efecto, la irrupción en la segunda mitad del siglo XX de la *perspectiva victimológica* en el ámbito de las ciencias penales supuso un progresivo giro copernicano en el modo de analizar el hecho delictivo que, hasta entonces, venía siendo explicado como el «producto unilateral de la decisión de un autor»[19]. De este modo, la Victimología, en cuanto ciencia criminológica centrada en la víctima del delito, sus elementos, su papel y, en especial, su contribución al surgimiento del delito[20], introdujo un cambio de paradigma de importantes consecuencias en el conjunto de las ciencias penales: desde la Criminología y el Derecho penal, hasta la Política criminal y el Derecho procesal penal.

La evolución en el modo de entender el significado y las consecuencias del comportamiento de la víctima en la responsabilidad penal del acusado ha sido magistralmente descrita por Vera Bergelson (2009)[21]. Así, según Bergelson, de acuerdo con un código binario simplista, la culpabilidad del acusado parecería presumir la inocencia de la víctima. De hecho, la percepción de las víctimas como protagonistas inocentes en el hecho delictivo –en el que se encuentran e interaccionan esa "pareja penal" (*penal couple*) compuesta por ofensores u ofensores y víctimas–,

---

[18] Cancio Melià, M. (2001). *Conducta de la víctima e imputación objetiva en Derecho penal*. J.M. Bosch editor, Barcelona.

[19] Silva Sánchez, J.M. (1989) ¿Consideraciones victimológicas en la teoría jurídica del delito? Introducción al debate sobre la victimodogmática, en *Criminología y derecho penal al servicio de la persona: libro homenaje al profesor Antonio Beristain*, (coord. por Enrique Echeburúa Odriozola, José Luis de la Cuesta Arzamendi, Iñaki Dendaluce Segurola), pp. 633-646. Herrera Moreno, M. (2006). Victimización: aspectos generales. En E. Baca, E. Echeburúa y J.M. Tamarit (coords.), *Manual de Victimología*, Valencia: Tirant lo Blanch, pp. 79-128.

[20] Ebert, "VerbrechensbekämpfungdurchOpferbestrafung?",*Juristenzeitung (JZ)* 1983, pp. 633-643.

[21] Bergelson, V. (2009).*Victims' Rights and Victims' Wrongs. Comparative Liability in Criminal Law*. Standford University Press.

se remonta a la Antigüedad y, de forma significativa, antecede a nuestro sistema de justicia penal. En numerosas culturas, la noción de víctima se hallaba fuertemente vinculada al sacrificio religioso, llegándose a utilizar, de hecho, la misma palabra para la víctima de un sacrificio y la víctima de un delito. Así, si aquellas criaturas que debían servir como víctimas del sacrificio debían ser puras, sin mancha alguna, del mismo modo se asociaba y se asocia todavía hoy que a toda víctima le corresponde la más plena inocencia. En ese contexto, de forma natural se entendía la intervención de la víctima en voz pasiva, como alguien que sufría un daño, *objeto* más que *sujeto* de un hecho delictivo.

Siguiendo a Bergelson, se debe partir de que, en realidad, el concurso de las víctimas debe entenderse, con frecuencia, como el papel propio de auténticos coautores (mejor, co-causantes) del daño que ellas mismas sufren. En efecto, las víctimas pueden participar en actividades riesgosas; aceptar que les inflijan dolor o daños; atacar o provocar a un tercero. En ocasiones, las víctimas no toman las debidas precauciones contra sus ofensores; o son ellas mismas ofensores. De hecho, con frecuencia –así lo muestra la investigación criminológica–, los ofensores de hoy son víctimas del mañana.

Así las cosas, la compleja dinámica interpersonal entre víctimas y ofensores que revisten muchos casos cotidianos requiere un análisis, también complejo, de un posible reparto de cuotas de responsabilidad, que puede afectar, en términos jurídico-penales, tanto a la relación de *imputación objetiva* como a la *desvaloración de la acción* y, de superarse positivamente los juicios de tipicidad y antijuricidad, incidir en la determinación de la pena. Más aún si, por ejemplo, nos referimos a delitos imprudentes y, de modo especial, si la estructura comisiva de éstos se desarrolla en comisión por omisión.

Si bien la jurisprudencia norteamericana parte de la máxima *Don't blame the victim*, no siendo, en principio, la posible culpa de la víctima una defensa completa o incompleta esgrimible, ello no debe implicar que se ignore en la definición del tipo penal la posible relevancia del comportamiento de la víctima. De hecho, en los últimos años ha habido un creciente desarrollo de las tesis victimodogmáticas que, en esa línea, introducen consideraciones correctoras a una visión unilateral del evento delictivo. Dicho de otro modo, el movimiento de defensa de los derechos de las víctimas se ha ocupado, fundamentalmente, de sensibilizar a la sociedad y a la comunidad política en su conjunto, tratando de obtener, tanto en el proceso de creación del Derecho como en el ámbito procesal, una mayor visibilidad y consideración de las víctimas. Éstas no podían seguir siendo *la parte olvidada*, que había sido apartada del proceso penal para

dotar de una mayor neutralidad a la función de hacer justicia, en tanto que la voz de las víctimas se consideraba relevante. Pues bien, las consideraciones victimodogmáticas son, en cierto modo, una extensión coherente de tal planteamiento: si la voz de las víctimas es relevante a efectos de aportar información sobre la otra cara del conflicto, por la misma razón debe entenderse que no solo su voz, sino también su conducta, debe tenerse en cuenta en la valoración del hecho objeto de enjuiciamiento, un hecho que es, en la mayoría de los casos, *cosa de dos*. En este sentido, el análisis de la conducta de la víctima en la dogmática penal ha sido denominado «the dark side of the moon of the victims' rights movement»[22].

Así, debe contemplarse el hecho delictivo–continúa Bergelson– como el resultado de una sinergia entre ofensor y víctima donde cada cual comparte una porción de la responsabilidad jurídica por las consecuencias negativas de su propio comportamiento. En sus propias palabras: «Si la víctima modifica su estatus moral y jurídico con respecto al ofensor, de forma voluntaria (mediante su consentimiento o la asunción de un riesgo) o involuntaria (por medio de un ataque a derechos reconocidos legalmente a terceros), los ofensores deberían estar en su derecho a oponer una justificación completa o incompleta, lo cual eliminaría o disminuiría su responsabilidad criminal» (p. 3).

En todo caso, pueden darse situaciones muy diversas que convendrá distinguir. A este respecto, Benjamin Mendelsohn–considerado, junto a Hans von Hentig, uno de los fundadores de la Victimología como rama independiente de la Criminología–, formuló con base en un estudio-cuestionario sobre sus clientes-víctimas (en su ejercicio como abogado) una tipología de víctimas que abarcaba diferentes grados de culpabilidad. En dicha clasificación, distinguía desde (1) víctimas completamente inocentes (por ej., un niño), hasta (2) víctimas a las que se atribuía la culpa en su totalidad (por ej., un ofensor que resultaba muerto por su víctima, actuando ésta en legítima defensa). Entre ambos extremos, Mendelsohn situaba tres tipos más de víctimas: (3) víctimas con una culpa menor, (4) víctimas tan culpables como el propio ofensor y (5) víctimas más culpables que su ofensor[23].

---

[22] Ortiz de Urbina Gimeno, I. (2008) Old Wine in New Wineskins? Appraising Professor Bergelson's Plea for Comparative Criminal Liability. *Pace Law Review* 28 (2008), 815-45.

[23] Mendelsohn, B. (1956). The Victimology.En *Etudes Internationales de Psycho-Sociologie Criminelle* 1 (1956).Schafer, S. (1977). *Victimology: The Victim and His Criminal*. Reston, Va: Reston Pub. Co.

III. ALGUNAS CONSIDERACIONES VICTIMOLÓGICAS APLICADAS AL CIBERESPACIO

Tras analizar el origen de la *perspectiva victimológica* y sus repercusiones en el ámbito jurídico-penal, me centraré en lo que sigue en la perspectiva victimológica en sentido estricto y aplicada al ciberespacio. Con el trascurrir del tiempo, al examinar la evolución de las contribuciones realizadas en el ámbito de la Victimología, se constata la existencia de un conjunto muy diverso de tipologías victimológicas o clasificaciones de tipos de víctimas en función de la perspectiva adoptada. Junto al enfoque tradicional centrado en la dinámica comisiva del delito, se fue enriqueciendo poco a poco la perspectiva de análisis, añadiéndose, por ejemplo, consideraciones de carácter psicológico, cultural o socioeconómico. De este modo, las tipologías basadas en una pluralidad de factores de riesgo, propensión o vulnerabilidad presentan actualmente la ventaja de su carácter multiaxial[24]. Siguiendo la clasificación propuesta por Herrera Moreno[25], la victimización en el ciberespacio se adaptaría plenamente, a mi modo de ver, a la tipología basada en la *vulnerabilidad contextual*, perspectiva que se centra en el análisis de la interacción de la víctima con un «entorno victimogenésico» como factor preponderante.

Ciertamente, la interacción entre ofensor y víctima en el contexto de los delitos cometidos en entornos virtuales posee características propias. Siguiendo la teoría de las actividades cotidianas[26], Miró Llinares[27] ha realizado un exhaustivo análisis de las modulaciones que en tal contexto experimentan los tres elementos que deben concurrir en un espacio y tiempo determinados para que tenga lugar un hecho delictivo: un *ofensor motivado* y una *víctima adecuada* (a la motivación del ofensor), junto ala ausencia de *guardianes capaces*. Su tesis principal es que el papel que

[24] Herrera Moreno, M. (2006). Victimización: aspectos generales. En E. Baca, E. Echeburúa y J.M. Tamarit (coords.), *Manual de Victimología*, Valencia: Tirant lo Blanch, pp. 79-128.

[25] Herrera Moreno, M. (1996). *La hora de la víctima. Compendio de Victimología*. Publicaciones del Instituto de Criminología de la Universidad Complutense. Madrid: Edersa.

[26] Cohen, L.E. y Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* 44: 588-608.

[27] Miró Llinares, F. (2011). *La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. Revista Electrónica de Ciencia Penal y Criminología, núm. 13-07.Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons.

juega la propia víctima en el ciberespacio resulta mucho más determinante, en comparación con lo relativo a su vida cotidiana en el espacio físico-corporal, en la medida en que al incorporar determinados bienes y esferas de su personalidad es ella misma la que crea los márgenes genéricos del ámbito del riesgo al que va a someterse[28]. Y aún más relevante: en cuanto a la teórica delimitación de los posibles riesgos a que se expone la víctima debe señalarse que, por las particularidades de los entornos virtuales, dicha exposición al riesgo se caracteriza por su naturaleza difusa y las dificultades que, con frecuencia, encuentra el propio interesado en el control de la información; su vocación de permanencia en el tiempo (por las dificultades de borrar las huellas digitales una vez se ha cruzado ese umbral digital); y su proyección altamente expansiva al abrirse a un círculo de potenciales ofensores mucho más amplio y diverso.

Es decir, parece que la explicación, fenomenología e implicaciones de una misma figura de delito, sobre todo desde la perspectiva de la víctima, sigue patrones y características diversas cuando el delito se comete en el ciberespacio (piénsese, por ejemplo, en términos de *bullying* o *cyberstalking*, y en cómo la víctima se puede hallar permanentemente expuesta al acosador).Como señala Miró Llinares, siguiendo la acertada metáfora de Grabosky, la cuestión radica en determinar en qué medida el ciberdelito, frente a su equivalente figura delictiva clásica, es *old wine in new bottles*; es decir, (i) si estamos frente a un tipo de delincuencia esencialmente nueva y respecto de la cual no son válidas las teorías criminológicas aplicables al delito tradicional llevado a cabo en el espacio físico-corporal; o,más bien, (ii) se trata del mismo delito a pesar de reunir, en función del contexto (virtual o físico), aspectos diferentes, pero para los que son válidas las mismas teorías y los mismos instrumentos utilizados en el espacio físico; o, por último, (iii) si puede tratarse de «una criminalidad con elementos configuradores idénticos pero que se ven afectados, de forma esencial, al plasmarse en el ciberespacio, de modo tal que ello puede influir significativamente en la explicación del delito y, por tanto, en su prevención»[29].

De este modo los delitos clásicos, ya sean contra el patrimonio (como el robo o la estafa) o contra las personas (delitos contra el honor, la libertad sexual o la intimidad), revisten perfiles y singularidades que afectan de modo considerable al *modus operandi* y sobre todo, por lo que aquí interesa,

[28] Miró Llinares, F. (2012), *op. cit.*, p. 263.

[29] Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13-07.

al principal protagonista del hecho delictivo, aumentando con ello intensamente la exposición de la víctima. En palabras de Max Estrella, personaje central de *Luces de Bohemia*, podría decirse que «[l]os héroes clásicos han ido a pasearse en el Callejón del Gato […]. Los héroes clásicos reflejados en espejos cóncavos dan el Esperpento»[30]. La deformación grotesca, esperpéntica, con que se presenta el ofensor en la red, deformando su imagen real, viene a alterar las circunstancias normales de interacción entre las personas y, con ello, los patrones delictivos clásicos, de tal forma que se hace necesaria una modulación significativa de las categorías criminológicas y dogmáticas a la hora de analizar, de hecho, las mismas figuras de delito.

En efecto, como veremos, la relación entre ofensor y víctima, mediada por "máscaras virtuales", facilita al ofensor el recurso a apariencias engañosas, técnicas de camuflaje y de manipulación, y potencian en la víctima una serie de déficits cognitivo-conductuales que incrementan notablemente los riesgos de victimización. Así, junto a la rapidez, intensidad y extensión inusitadas con que se cometen los delitos en la red, las interacciones a través del ciberespacio fomentan un mayor anonimato, factor criminógeno de primera magnitud; una mayor impulsividad, irreflexión e ingenuidad en la toma de decisiones por parte de la víctima, presa, con frecuencia, de un consumismo impulsivo; una acusada pérdida del sentido de intimidad, de la que se deriva una tendencia a proporcionar datos personales a extraños de forma incontrolada; un mayor exhibicionismo de los sentimientos y de la corporeidad, fuente de una mayor imprudencia que actúa como fuerza de atracción (ya sea de acosadores sexuales o de estafadores); y una multiplicación de los efectos denigrantes derivados de una victimización padecida ante un escaparate global.

En relación a las máscaras que proporcionan los entornos virtuales, pueden presentarse dificultades en la delimitación y distinción entre la persona real (el yo-real) y la persona digital (el yo-digital). Con base en el origen etimológico greco-latino del término *persona*, un individuo puede tener dos máscaras o personalidades, una encarnada corporalmente y otra virtual–ajena a dicha dimensión corporal–, representada a través del lenguaje, estando o no asociada a una imagen visual. En cualquier caso, el individuo puede sentirse igualmente dañado cuando una de las dos máscaras es objeto de ataque[31]. No obstante, debe señalarse una diferencia que me parece significativa entre una realidad completamente virtual (en el que la disociación entre el yo-digital y el yo-real llega a ser comple-

[30] Valle Inclán, 1920: Escena XII.

[31] Guinchard, A.(2010). Crime in virtual worlds: The limits of criminal law. *International Review of Law, Computers & Technology*, Vol. 24, No. 2, July 2010, p. 178.

ta) y una realidad virtual en la que la vinculación con la realidad físico-corporal sigue presente, pese a ser muy tenue en ocasiones. Con todo, la línea divisoria entre una y otra categoría no es en absoluto clara, constituyendo el elemento clave a efectos criminológicos y jurídicos, el hecho de que las consecuencias de las acciones tengan un *impacto tangible* en la vida real de las víctimas. A este respecto, siguiendo de nuevo a Guinchard se puede distinguir entre aquellos delitos que requieren una afectación *físico*-corporal ineludible (*physicality*), como un asesinato o una violación, de aquellos otros que no lo requieren (como los delitos de fraude, acoso moral o sexual, o injurias y calumnias). Todo ello lleva a plantearse si los estándares jurídicos tradicionales –las categorías dogmáticas de la teoría del delito– necesitan ser modificados para tomar en cuenta que, de hecho, los delitos pueden cometerse en un escenario virtual de una forma ciertamente distinta[32].

En las líneas que siguen, trataré de esbozar algunas de las principales características delictivas en razón del contexto que, en mi opinión, deberían tenerse en cuenta al abordar la cuestión victimológica en relación, sobre todo, con las medias de autoprotección de las víctimas en entornos virtuales. Para ello, me centraré sobre todo en las implicaciones que introduce la perspectiva victimológica en las *medidas de prevención del delito* (perspectiva criminológica), refiriéndome tangencialmente a las consecuencias de dicho enfoque en la *aplicación de algunas categorías de la teoría del delito* (perspectiva jurídico-penal), todo ello cuando el espacio en el que tiene lugar el hecho delictivo escapa a la relación directa en el espacio físico-corporal.

IV. LUGAR Y DELITO: ARQUITECTURAS DIGITALES, CONVERGENCIA DE ESPACIOS Y DIVERGENCIA ESQUIZOFRÉNICA

En la era digital, las actividades cotidianas de las personas, especialmente las de los *grown up digital*[33], se desenvuelven en una porción de tiempo cada vez mayor a través de arquitecturas digitales. De hecho, la línea divisoria entre lo virtual y lo físico-corporal no siempre es nítida. En la

[32] Smyth, S.M.(2009). Back to the Future: Crime and Punishment in Second Life. *Rutgers Computer & Technology Law Journal*, Vol. 36, 1. p. 22.

[33] Tapscott, D. (2008). *Grown Up Digital: How the Net Generation is Changing Your World*. McGraw-Hill.

Se suele utilizar la expresión "nativos digitales" (*born digital* o *digital natives*) para designar a quienes ya han nacido inmersos en la era digital, si bien me parece preferible referirse a la generación que ha madurado y crecido de hecho en un entorno y cultura digital (*grown up digital* o *net generation*).

actualidad, los adolescentes se encuentran cada vez más permanentemente conectados a través de las TIC; expresan su identidad e interactúan entre sí con una sorprendente naturalidada través del espacio virtual, en el que proyectan incluso con mayor intensidad manifestaciones de intimidad.

¿Qué distingue, pues, ambos espacios de relación social y comunicación? Sin duda, el elemento diferenciador de ambas realidades radica en la "contigüidad" físico-corporal[34]. Pero la realidad virtual sigue avanzando y, en algunos casos, el contacto corporal entre las personas llega a lograrse, en términos prácticos, de forma similar a la contigüidad física, a pesar de la distancia. Piénsese, por ejemplo, en las operaciones quirúrgicas a distancia y los avances en telemedicina. Más aún, con el nacimiento de mundos (enteramente) virtuales (*Virtual Worlds*) a partir de la creación en junio de 2003 de *Second Life* se ha abierto un nuevo ámbito de interacciones sociales –y, por tanto, de posibles delitos–, que presenta cuestiones jurídicas relevantes.

Second Life, en efecto, existe: se trata de un lugar tridimensional en el que sus habitantes virtuales pueden comprar, trabajar, explorar un sinfín de nuevas oportunidades; toda una comunidad virtual se presenta como un lugar abierto en el que cada uno puede crear su propia personalidad y decidir su propio destino, donde existe una economía propia en la que se opera con moneda propia (*Linden dollars*), convertible en dólares americanos, y donde las personas pueden mantener interacciones de todo tipo[35]. Esta meca virtual provee de este modo también nuevas oportunidades para el delito que pueden tener un alcance global, ser de muy bajo coste y aprovecharse desde una prácticamente completa anonimidad, no limitándose los posibles daños infligidos a terceros al mundo virtual, sino que pueden traspasar sus fronteras y causar daños significativos a las víctimas en su vida real[36].

Pero volvamos a las interacciones más usuales en entornos virtuales. Lo relevante en ellas es que existe una relación humana entre personas reales. Por este motivo, Miró Llinares se refiere al ciberespacio como «un lugar de comunicación que no tiene una naturaleza física primaria, sino esencialmente relacional», en el que se produce una contracción total del espacio (de las distancias) y, a la vez, la dilatación de las posibilidades de encuentro y comunicación entre personas[37]. No hay duda, pues, de que no podemos

[34] Gutiérrez Puebla, J.(1998). Redes, espacio y tiempo. *Anales de Geografía de la Universidad Complutense*, núm. 18, pp. 65-86.

[35] Guinchard (2010), *op. cit*.

[36] Smyth (2009), *op. cit*.,p. 21.

[37] Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13-07.

ya referirnos al "mundo virtual"[38] frente al "mundo real", pues ambas dimensiones forman parte de la realidad de las cosas. Pease (2001), de forma gráfica, contrapone el *cyberspace* al *meatspace*: lo único que distingue ambos espacios es la presencia del sujeto en carne y hueso, de cuerpo presente, a pesar de que los efectos de esa relación a través del ciberespacio pueden llegar a incidir, en ocasiones, en la corporeidad de la víctima.

Desde la significativa aportación de Katyal (2003)[39], es un lugar común referirse a la arquitectura digital como factor criminógeno, sobre todo por las condiciones de anonimato que lleva aparejada, y a la necesidad de arbitrar estrategias de prevención del delito en función del contexto[40]. Así, con base en la contribución, anterior en el tiempo, de Lawrence Lessig[41]–cuya idea-fuerza consistía en identificar la arquitectura como un elemento clave que podía constreñir el comportamiento online–, han venido sucediéndose desde entonces enfoques y acercamientos interesantes sobre espacio, geografía y ciberdelito[42].

A este respecto, ¿qué diferencia existe entre engañar a través de la red o hacerlo de cuerpo presente; entre acosar siguiendo a la víctima por todas partes cuando sale de su hogar o hacerlo a través del ciberespacio; o entre espiar a una persona en una situación íntima mediante contacto visual directo o realizarlo a través de la *webcam* de su propio ordenador, en el que previamente se ha instalado un troyano?

Como señala Grabosky[43], ciertamente «la emoción del engaño que caracterizó la introducción del caballo de Troya sigue vigente en la creación de sus descendientes digitales»; pero lo que ha cambiado son las facilidades con que cuentan los ofensores, su *modus operandi*, y el consiguiente aumento del riesgo de victimización. Es decir, el cambio se ha operado en las condiciones de oportunidad: los ofensores encuentran víctimas adecuadas en circunstancias realmente propicias.

---

[38] De hecho, según el Diccionario de la Real Academia Española la voz "virtual" proviene del latín, concretamente del término *virtus–is*: fuerza, virtud, y en su primera acepción se define como: «1. adj. Que tiene virtud para producir un efecto, aunque no lo produce de presente, frecuentemente en oposición a efectivo o real».

[39] Katyal, N.K. (2003). Digital Architecture as Crime Control, 111 *Yale Law Journal* 1039.

[40] Agustina, J.R. (2009). Arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual. *International E-Journal of Criminal Sciences*, núm. 3 (2009).

[41] Lessig, L. (1999). *Code and Other Laws of Cyberspace*. NY: Basic Books, pp. 4-14.

[42] Véase, en extenso, Miró Llinares, F. (2012) *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons.

[43] Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies* 10, 248.

Sin embargo, la unidad lograda en virtud de la convergencia entre el espacio físico-corporal y el espacio virtual a la que nos hemos referido, contrasta con la tendencia a la desfragmentación del yo, dando lugar a conductas y perfiles de usuarios a través de las TIC, más o menos patológicos, que presentan síntomas de cierta *esquizofrenia digital*[44].Se produce pues, como veremos, una tendencia a la divergencia o disociación entre el yo-digital y el yo-real, en la medida en que por las circunstancias del contexto virtual la persona puede sentirse llamada a llevar una doble vida en la red, extraña a su vida social en sus actividades cotidianas en el espacio físico-corporal. Veamos a continuación algunas manifestaciones.

V. ENTORNOS VICTIMÓGENÉSICOS Y PERFILES VICTIMOLÓGICOS

A) ONLINE DISINHIBITION EFFECT

Una primera característica de las víctimas en el ciberespacio hace referencia al efecto desinhibidor que el contexto ejerce sobre las mismas. Diversas investigaciones sobre el modo de comportarse de los usuarios habituales de Internet señalan cómo las personas dicen y hacen cosas en el ciberespacio que no dirían ni harían en circunstancias ordinarias en sus relaciones *face-to-face*[45]. Las personas se sienten así, en contextos *online*, menos constreñidas, más sueltas y se expresan de una forma mucho más abierta que en sus relaciones directas. El fenómeno ya es tan generalizado que se ha comenzado a denominarlo como un "efecto desinhibidor" del ciberespacio sobre la conducta de las personas (*online disinhibition effect*). En cierto modo, añadiría, se podría hablar también de una tendencia hacia la *esquizofrenia digital*, según la cual las personas se ven empujadas a llevar una doble vida en la red, tendencia que está fuertemente reforzada (aunque no siempre) por las condiciones de anonimato y la consiguiente desfragmentación o desdoblamiento de la persona, dando lugar a un *yo-digital* distinto del *yo-real*.

La desinhibición puede dar lugar a ciertos efectos positivos o benignos, pero puede ir acompañada también de efectos negativos o, en oca-

[44] Entiéndase la expresión en un sentido metafórico-coloquial. Además, como es sabido, a pesar de su etimología, la *esquizofrenia* no es lo mismo que el *trastorno de identidad disociativo* (o «trastorno de personalidad múltiple», o de «doble personalidad»), con el que ha sido frecuentemente confundida.

[45] Suler, J. (2004) The Online Disinhibition Effect. *Cyberpsychology & Behavior*, Volume 7, Number 3., 2004.

siones, perversos. Por ejemplo –señala Suler–, verter palabras hostiles al participar en un *chat* puede tener efectos terapéuticos de desahogo para algunas personas. En una relación vía e-mail en la que de forma creciente se va abriendo paso a una comunicación de la intimidad, la gente puede rápidamente llegar a revelar información personal, lamentándose con posterioridad de ello y llegando a sentirse de hecho expuesta, vulnerable o avergonzada. Puede tomar cuerpo una relación de intimidad de forma excesivamente rápida e incluso falsa que, por ello, con posterioridad destruye dicha relación cuando una de las dos partes siente aturdimiento, ansiedad o desconcierto. «¿Qué elementos del ciberespacio conducen a ese debilitamiento de las barreras psicológicas que bloquean los sentimientos y necesidades escondidas?» –se pregunta Suler.

Este autor, desarrollando las características de una *psicología para el ciberespacio*, enumera los siguientes elementos: (1) *anonimidad disociativa*: la posibilidad de no revelar la propia identidad conlleva que, en virtud del anonimato, la persona pueda garantizar que no se vincule su actividad *online* con su persona en la vida "real", disociando así ambas identidades; (2) *invisibilidad*: el hecho de que las personas puedan navegar a través de la red, entrando en páginas web o páginas de *chat* sin ser no solo identificados sino también sin que el resto de usuarios perciban su presencia, impulsa que se atrevan a visitar lugares que, de otro modo, nunca visitarían –sobre todo por vergüenza y por las consecuencias en su propia reputación–; (3) *asincronicidad*: en las comunicaciones en el ciberespacio muchas veces la interacción no se produce en tiempo real, al menos no necesariamente. Este hecho proporciona una mayor capacidad de pensar y editar la forma de presentarse, proporcionando mayor seguridad a los adolescentes[46]; y facilita que puedan darse situaciones en las que, tras una mayor reflexión o ante un momento de impulso, la persona llegue a escribir un mensaje muy personal, hostil o cargado de emociones y huir, fenómeno que podría describirse como un "*emotional hit and run*"; (4) *introyección solipsística*: fruto de la ausencia de datos fiables sobre la otra persona, puede producirse un efecto psicológico por el que el sujeto asigna características y rasgos a la persona o personas con las que interactúa en la red que, en realidad, son fruto de la propia imaginación. Las fantasías de la imaginación, pudiéndose dar también en la vida "real", se ven potenciadas de forma considerablemente desinhibida en la red; (5) *imaginación disociativa*: de forma consciente o inconsciente, los internautas pueden llegar a percibir que los personajes imaginarios que ellos mismos

[46] Valkenburg, P.M y Peter, J. (2011). Online communication hmong adolescents: An integrated model on its attraction, opportunities, and risks. *Journal of Adolescent Health*, 48, 121-127.

"crearon" existen en un espacio diferente; que su yo-digital junto a esas otras personas *online* viven en otra dimensión, en sus sueños, separada de las exigencias y responsabilidades de su vida "real". De este modo se produce una fragmentación o disociación entre el mundo de ficción *online* y los hechos de su vida real *offline*; (6) *minimización del status y autoridad*: en Internet todo el mundo parte, en cierto modo, de la misma posición, al estar todas las personas (aunque sean famosas o detenten alguna posición de autoridad), igualmente accesibles; y, por otro lado, el hecho de estar en la red conlleva que las personas con un cierto status o autoridad puedan perder los atributos visibles que en el mundo "real" le distancian del resto de mortales, con los efectos desinhibidores que ello conlleva.

Los efectos desinhibidores del ciberespacio que se acaban de describir elevan, lógicamente, las probabilidades de que los usuarios incurran en conductas de riesgo y acaben siendo cibervictimizados. La desinhibición lleva, pues, a la víctima a cruzar el *umbral de riesgo*. En este sentido, me he referido en otro lugar a los riesgos inherentes a la práctica del *sexting*[47], como ejemplo paradigmático de cruzar una *línea roja* que abre las puertas a un elevado riesgo de victimización («Sexting as a Threshold for Victimization»). En efecto, al margen de la compleja discusión acerca de si ciertas conductas de *sexting* pueden considerarse ya en sí mismas penalmente relevantes (por constituir un delito de distribución de pornografía infantil), de lo que no hay ninguna duda es de que el *sexting* constituye un predictor importante de eventuales formas de cibervictimización[48]. Baste señalar que el solo hecho de poner en manos de un tercero, o de un círculo íntimo de personas, imágenes de contenido sexual explícito abre las puertas a conductas de extorsión, chantaje, conductas vengativas o simplemente frívolas, por las que dicho material gráfico o audiovisual puede acabar siendo difundido a un número ilimitado de personas (véase, a continuación, la *Tabla de riesgos y delitos derivados de practicar sexting*):[49]

[47] Agustina, J.R. (2012). Analyzing Sexting from a Criminological Perspective. Beyond Child Pornography Issues: Sexting as a Threshold for Victimization. In Pauline C. Reich (Eds.), *Cybercrime & Security*, West, Thomson Reuters, Section 4:4, 64-96.

[48] Reyns, B.W., Burek, M.W., Henson, B., y Fisher, B.S. (2011b). The unintended consequences of digital technology: exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice*, 2011, 1–17.

[49] Agustina, J.R. (2012),op. cit.,p. 93.

Table 7: *Crimes and risks derived from sexting*

Embarrassment
Privacy crimes
Defamation
Bullying or cyber-bullying
Sexual harassment
Blackmail or extortion
Grooming
Sexual coercion
Offline sexual abuse or rape
Homicide
Suicide

B) Víctimas ingenuas e irreflexivas

Como han señalado Bossler y Holt[50], las teorías criminológicas con un enfoque situacional (es decir, las teorías de las actividades cotidianas y de los estilos de vida, así como el resto de teorías de la oportunidad) han dominado el campo de la Victimología. Esto ha llevado a que, lamentablemente, las teorías orientadas al individuo han sido prácticamente ignoradas en los estudios de victimización.

Junto al efecto desinhibidor estructural o situacional que influye de forma general en la conducta *online*, conviene tener presente la especial incidencia de la cultura digital en las generaciones que ya han crecido y se han desarrollado desde su primera infancia en un entorno digitalizado. A este respecto, ¿cómo interactúan los adolescentes hoy en día en sus actividades cotidianas? Siguiendo la máxima cartesiana (*Cogito ergo sum*, es decir, *pienso, luego existo*), se podría formular la siguiente pauta cultural en las generaciones *grown up digital*:"*I twit, I post, I blog –therefore, I am!"*. Es decir, al efecto de desinhibición descrito, debe sumarse el hecho de que los adolescentes pasan en la actualidad muchas horas al día entre SMS's, *whatsap's* y *twits*, navegando en Internet, participando en redes sociales o *chats*, o *colgados* del móvil. A pesar de la escasez de estudios empíricos acerca de qué tipo de conductas en particular entrañan especiales riesgos[51], como señala este autor, la mayoría de estudios de victimización *online* se centran en los jóvenes, "a cuya mejor tutela la sociedad es especialmente sensible", por un mo-

[50] Bossler, A.M. y Holt, T.J. (2010).The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*38 (2010) 227–236.

[51] Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons.272-273.

tivo bien claro: son los jóvenes los que de forma más generalizada usan las TIC y desarrollan sus actividades cotidianas en el ciberespacio. No obstante, habrá que ver si son siempre los jóvenes esa *víctima adecuada* que pretende encontrar todo *delincuente motivado* y, en ese sentido, habrá que distinguir en función de los intereses que mueven a los ofensores. Así, parece razonable, como por otro lado confirman en su investigación Ngo y Paternoster[52], que a mayor edad, mayores probabilidades de sufrir una infección de *malware* o ser objeto de mensajes injuriosos o denigrantes. De todos modos, no existen estudios con muestras con un intervalo de edad amplio que permitan diferenciar por edades, habiéndose realizado la casi totalidad de las investigaciones sobre muestras obtenidas en poblaciones juveniles, universitarias o en últimos cursos de enseñanza secundaria o bachillerato[53].

En todo caso, el efecto desinhibidor en la persona (derivado de un entorno digitalizado) genera una aceleración de la conducta en una dinámica en el uso de las TIC que reviste con frecuencia *tintes compulsivos*, y se traslada a la esfera decisional del sujeto en términos de una mayor confianza o relajación en sus interacciones (ingenuidad) y en una ausencia de reflexividad en sus procesos de toma de decisiones (irreflexividad). Tales rasgos conductuales nos acercarían así a afirmar que el ciberespacio, de hecho, puede poseer un efecto determinante en los niveles de autocontrol del individuo. Por tanto, la aplicación de las tesis principales de la teoría del autocontrol[54] deberían recibir una mayor atención para determinar en qué medida los mayores riesgos de cibervictimización pueden derivarse de una más pobre capacidad de autocontrol, si bien aplicando el test de autocontrol a las víctimas y no a los delincuentes–público al que se dirigía en primer lugar dicha teoría–. Al respecto, es de obligada consulta el importante trabajo sobre autocontrol y cibervictimización de Bossler y Holt[55], en el que se plantea la necesidad de una mayor exploración de dicha hipótesis. Y –de confirmarse al menos para determinados grupos de cibervíctimas–, ello pondría de relieve la importancia de la educación de los menores en el uso de las TIC, factor éste de una

[52] Ngo, F. y Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, vol. 5, núm. 1.

[53] Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons. Reyns, B.W., Henson, B., y Fisher, B.S. (2011a). Being pursued online: applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38, 1149–1169.

[54] Gottfredson, M.R. y Hirschi, T. (1990). *A General Theory of Crime*. Standford, CA: Standford University Press.

[55] Bossler, A.M. y Holt, T.J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice* 38 (2010) 227–236.

enorme relevancia y que, sin duda, merecería un primer lugar en las estrategias de prevención de la cibervictimización.

No me resisto a apuntar aquí las posibilidades de rendimiento que podría tener en lo aquí tratado la *teoría de la acción situacional* de Wikström[56]. Aunque este criminólogo no ha aplicado (todavía) su teoría a la ciberdelincuencia, me parecería sumamente interesante adaptar al ciberespacio los constructos de su teoría relativos al modo en que interaccionan las percepciones morales del sujeto en función del entorno cultural y situacional. Piénsese no solo en el efecto desinhibidor referido, sino en las pautas culturales y normativas, ciertamente cambiantes de una a otra sociedad, por ejemplo en materia de derechos de *copyright* o de protección de datos.

VI. ESTRATEGIAS DE PREVENCIÓN Y AUTOPROTECCIÓN DE LA VÍCTIMA EN EL CIBERESPACIO

Pasamos ahora a analizar los problemas que hemos ido tratando desde la perspectiva de la prevención. Como es sabido, la literatura criminológica distingue tres tipos de enfoque en la prevención del delito[57], que lógicamente pueden y deben adaptarse a los ciberdelitos. Así, por ejemplo, en relación con las estrategias de *prevención primaria* en el ciberespacio se podrían apuntar distintos instrumentos y medidas dirigidos a fortalecer o corregir déficits en la población de usuarios de las TIC en su conjunto, fomentando una mayor educación en el uso de Internet[58]; una mayor conciencia en los peligros que conciernen a la pornografía en Internet[59]; o un fortalecimiento de la cultura de la privacidad acorde con el escenario actual.

Desde el punto de vista de la *prevención secundaria*, se podrían diseñar políticas concretas encaminadas a atender las necesidades y corregir los déficits de prevención de *concretos grupos de riesgo*, relativos tanto a

---

[56] Wikström, P.-O.H. (2006) Individuals, settings, and acts of crime: Situational mechanisms and the explanation of crime. In Wikström y Sampson, *The explanation of crime: Context, mechanisms and development*, Cambridge University Press, pp. 61-107.

[57] Tonry, Michael; Farrington, David P. (1995) Strategic Approaches to Crime Prevention.19 *Crime & Justice* 1.

[58] Marcum, C.D. (2012). Adolescent Online Victimization and Constructs of Routine Activities Theory. In Jaishankar, K (Ed.): *Cyber Criminology. Exploring Internet crimes and criminal behavior*, CRC Press, Boca Ratón, 2011.

[59] Eberstatd, M. y Layden, M.A., Witherspoon Institute (ed.) (2011). Los costes sociales de la pornografía. Una exposición de hallazgos y recomendaciones, en *La pornografía y sus efectos sociales y criminógenos. Una aproximación multidisciplinar*, J.R. Agustina (dir.), Social Trends Institute (ed.), Colección Actualidad Criminológica y Penal, BdeF–Edisofer.

ofensores como a víctimas potenciales. En este sentido y con dicha finalidad, por ejemplo, Wolak et al. [60] han descrito los factores que identifican ciertas poblaciones vulnerables en relación a la cibervictimización sexual: (1) unas relaciones conflictivas o pobres con los padres; (2) circunstancias personales tendentes a la soledad y depresión; (3) una orientación sexual dubitativa como predictor de conductas de riesgo; (4) o la falta de conciencia de las propias víctimas respecto a su propia victimización.

Finalmente, desde un enfoque de *prevención terciaria* se podrían definir programas específicos de tratamiento de ofensores y víctimas *online*. Sin duda, algunas características de tales ofensores y víctimas pueden ser comunes, pero ello no resta importancia a la necesidad de un enfoque específico en función del tipo de delincuencia y victimización en el ciberespacio. De este modo, parece razonable diseñar específicos programas de tratamiento para pedófilos o programas de educación en casos de *sexting*. En relación a estos últimos, en Estados Unidos ya se han desarrollado y aplicado instrumentos específicos (véase, entre otros, el programa *Before you Text* reseñado en la bibliografía). Otro tanto podría decirse de los programas dirigidos a la recuperación de las víctimas.

Junto a los tres enfoques preventivos que se acaban de referir, desde hace unas décadas han emergido con fuerza distintas propuestas y medidas de intervención en el ambiente donde tienen lugar los delitos, y que han recibido el nombre de *técnicas de prevención situacional*. Se trata de medidas de contenido y enfoque muy diverso que se derivan de los postulados de las teorías de la oportunidad y cuyo objetivo principal es la reducción de oportunidades mediante la modificación de las condiciones ambientales.

Tras distintas versiones del catálogo estándar de técnicas de prevención situacional (en adelante, SCP, por sus siglas en inglés: *Situational Crime Prevention*), Cornish y Clarke[61] fijaron un conjunto de 25 técnicas de SCP que se han venido aplicando a concretos *problemas delictivos* para orientar el trabajo policial. Así encontramos un buen número de guías muy concretas para diagnosticar e intervenir sobre concretos fenómenos delictivos en la página web del *Center for Problem Oriented Policing*. No obstante, a pesar del desarrollo alcanzado, dichas técnicas se han aplicado, hasta la fecha, principalmente

[60] Wolak, J., Finkelhor, D., y Mitchell, K.J. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, 35, 424.e11– 424.e20.

[61] Cornish, D. y Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In: M.J. Smith and D. Cornish (eds.) *Theory for Practice in Situational Crime Prevention*, Vol. 16. Monsey, NY: Criminal Justice Press, pp. 41–96.

a entornos no virtuales[62]. Junto a los trabajos de Reyns, no obstante, comienzan a surgir instrumentos específicos orientados a prevenir ciberdelitos, como el *cyberstalking*, *cyberbullying*, *sexting*, *grooming*, o la pornografía infantil en Internet[63].

Tabla 1
Veinticinco medidas de prevención situacional de Cornish y Clarke (2003)

AUMENTAR EL ESFUERZO	AUMENTAR EL RIESGO	DISMINUIR GANANCIAS	REDUCIR PROVOCACIONES	ELIMINAR EXCUSAS
Entorpecer objetivos	Aumentar el número de guardianes	Ocultar objetivos	Reducir frustraciones/estrés	Establecer reglas
Controlar accesos	Facilitar la vigilancia	Desplazar objetivos	Evitar disputas	Fijar instrucciones
Controlar salidas	Reducción del anonimato	Identificar la propiedad	Reducir la excitación emocional	Alertar la conciencia
Desviar trasgresores	Introducir "gestores" de sitios	Trastornar los mercados delictivos	Neutralizar la presión del grupo de referencia	Asistir la conformidad
Controlar facilitadores	Reforzar la vigilancia formal	Eliminar beneficios	Disuadir imitaciones	Controlar las drogas y el alcohol

En este contexto, resulta especialmente remarcable el trabajo, al que ya nos hemos referido con anterioridad, de Miró Llinares, en el que presenta un conjunto de medidas concretas para la prevención de la ciberdelincuencia desde el enfoque situacional[64].En otro lugar, por exceder las pretensiones, más generales, del presente capítulo, desarrollaré un comentario más amplio de dicho conjunto de medidas –que se apuntan en la Tabla que aparece a continuación–, sin perjuicio de señalar aquí algunas breves observaciones.

---

[62] Reyns, B.W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, 12, 99-118.

[63] Wortley, R. y Smallbone, S. (2012). *Internet Child Pornography: Causes, Investigation, and Prevention*. Praeger: California, Colorado, England.

[64] Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 203-216.

Tabla 2
Veinte tipos de medidas de prevención situacional de la cibercriminalidad de Miró Llinares (2012)

REDUCCIÓN DEL ÁMBITO DE INCIDENCIA	AUMENTAR EL ESFUERZO PERCIBIDO	AUMENTAR EL RIESGO PERCIBIDO	DISMINUIR LAS GANANCIAS PERCIBIDAS	ELIMINAR EXCUSAS
No introducir objetivos; Separación de discos duros con acceso y sin acceso al sistema; sistemas de control parental; filtros de contenido; controladores de seguridad ActiveX; noacceso a *chat rooms (grooming)*.	Controlar el acceso al sistema Firewall; actualización de los sistemas operativos; claves de acceso al sistema; claves de acceso a las redes; renovación de claves; sistemas de perfiles en redes sociales.	Aumentar el número de guardianes Moderadores de foros; sistemas Echelon, Enfopol, Carnivore y Dark Web.	Ocultar objetivos; Utilización de sistemas de encriptación; ocultar datos personales en redes sociales; no utilización de claves bancarias; perfeccionamiento sistemas e-comercio.	Establecer reglas. Armonización internacional del Derecho; Netiquette.
Identificación de zonas de riesgo; Campañas de información sobre riesgos; aviso en red de infección de *spam;* sistemas de listas blancas y negras de web y *spam;* Identificación de *bots*.	Detectar e impedir el ataque Antivirus; antispyware; antispam; sistemas de control de banca electrónica.	Reducción del anonimato Identificar las IP; registro en foros webs; sistemas de identificación del usuario; identificación y autentificación biométrica.	Desplazar objetivos; Discos duros extraíbles; sistemas de pago alternativos (PayPal); cambio de direcciones web, direcciones de dominio y demás	Fijar instrucciones. Avisos web de licencias: *copyright* y *copyleft;* avisos sobre privacidad en redes sociales

ISSN: 0210-4059

Descontaminación/ limpieza de residuos Borrado y destrucción de virus latentes; desinfección de *bot*.	Retirar transgresores Cierre de webs; solicitud de retirada de contenido ilícito; mecanismos de denuncia en redes sociales; cortar el acceso a una IP.	Reforzar la vigilancia formal Control de webs a través de *proxy;* equipos especializados de persecución del cibercrimen.	Eliminar beneficios Persecución a compradores de contenidos ilícitos; persecución del blanqueo capitales.	Fortalecer la conciencia moral Concienciación en materia de propiedad intelectual; reforzar moralmente los negocios lícitos
Separación de objetivos Internet2 creación de sub-redes locales de seguridad.	Controlar facilitadores Obligaciones de vigilancia para IPPS; control de datos por Rss.	Facilitar la vigilancia Mejora de los sistemas de identificación de IP´s; reconstrucción de la arquitectura con fines defensivos	Trastornar los mercados delictivos Ofrecer sistemas de intercambio de archivos económicos (*Spotify* y más); control de páginas de descarga directa de archivos.	Facilitar la conformidad Nuevos modelos de negocio (*Apple*); competiciones legales de *Hacker*; fortalecimiento del *software* libre

ISSN: 0210-4059

1) En relación a la primera columna *Reducción del ámbito de incidencia*, se podría avanzar mucho, sin duda, mediante la organización de cursos de educación en el uso de las TIC, en la misma línea que sugiere el interesante proyecto ROBERT *Risktaking Online Behaviour Empowerment Through Research and Training*; o algunos programas educacionales que se han puesto en marcha en Estados Unidos a raíz del fenómeno del *sexting*, como el ya referido, diseñado en Texas, *Sexting Prevention Educational Program for Texas "Before you Text"* (ambas iniciativas se han reseñado en la bibliografía).

En el contexto de educar y concienciar a la población sobre los riesgos derivados de su estilo de vida *online*, y a modo de ejemplo, conviene llamar la atención sobre la utilización en redes sociales de sistemas de localización a través de GPS, mediante los que se puede seguir la pista, por ejemplo en *Facebook*, de los lugares en los que se halla presente o por los que transita una víctima potencial. Piénsese en que dicha localización, junto a la información que cada uno puede verter en la red sobre sus amigos, aficiones, intereses, etc., pueden ser utilizados por ofensores de distinta tipología, por ejemplo para saber cuándo se halla ausente la víctima de su domicilio o para localizarla en un punto determinado; o para dar una apariencia de veracidad al ofensor que pretende hacerse pasar por una persona que conoció en un lugar en el que estuvo la víctima, o que tiene amigos comunes, dándole señales confusas mediante toda esa información personal que la propia víctima ha publicado en su perfil.

Finalmente, en relación con la supervisión de los menores en el uso de las TIC podrían señalarse algunas medidas tendentes a reducir el ámbito de incidencia o exposición. Así, una recomendación que podría parecer *prima facie* contraproducente pero que se ha demostrado eficaz consiste en que los padres paguen a los menores la factura del móvil. *Trend Micro*, empresa dedicada a la seguridad de contenidos en Internet, así lo aconseja apoyándose en el estudio realizado por el *Pew Research Center*, cuyos resultados indican que el 7% de los adolescentes que pagan su factura envía *sexts*, frente al 3% de los que no se hacen cargo de los gastos (o sólo de una parte). Otra de las medidas propuestas por *Trend Micro* para los padres con hijos en edades comprendidas entre los 12 y los 17 años consiste en limitar el número de mensajes de texto que el adolescente puede enviar. En este sentido, el estudio señala que sólo el 8% de los adolescentes que practican *sexting* tienen restringido el número de mensajes de texto o de otros mensajes que pueden enviar, mientras que se ha encontrado que el 28% de aquellos que no lo practican tiene fijado un límite de mensajes por sus padres.

Otra medida que se orientaría en el mismo sentido consistiría en cubrir o inutilizar las *webcams* de los ordenadores en los hogares; o proporcionar a los menores teléfonos móviles que, sin dejar de ser relativamente atractivos, no dispusieran de cámara incorporada.

2) Respecto al conjunto de medidas dirigidas a *Aumentar el esfuerzo percibido* y a *Aumentar el riesgo percibido*, conviene resaltar una cuestión de especial trascendencia jurídica, a saber, la utilización de funcionarios policiales como *agentes encubiertos* y *agentes provocadores*. En efecto, aumentar el número de *guardianes capaces*, sobre todo si poseen conocimientos técnicos y criminológicos, puede suponer un aumento considerable del riesgo percibido por potenciales ofensores y, *ex post facto*, aumentar las probabilidades de éxito de las operaciones policiales –si bien, en ocasiones, más que en una actuación posterior al delito la policía interviene, como veremos, en la misma generación del delito con fines de finalización y aseguramiento de un curso de investigación o a modo de búsquedas aleatorias (*fishing expeditions*)[65].

A este respecto, actualmente en España, a diferencia por ejemplo de Estados Unidos, la utilización de *agentes encubiertos* contra la pornografía infantil y la pedofilia no goza de la cobertura jurídica necesaria. Según la legislación española actual (art. 282 bis LECrim), la figura del agente encubierto solo es admisible, mediante autorización judicial, para la investigación de "actividades propias de la delincuencia organizada". Además, dicho artículo delimita a qué tipo de delincuencia organizada puede aplicarse, y entiende por tal la asociación de tres o más personas de forma permanente o reiterada, para cometer alguno de los delitos enumerados en dicho artículo. En esa enumeración, además, no hay ningún tipo delictivo en el que de forma directa podamos incluir la pederastia (concretamente, el nuevo delito del art. 183 bis, denominado *grooming*): tan solo podría incluirse de manera indirecta en el delito de secuestro de personas o en el de prostitución y corrupción de menores, si es que se diera el caso. Pero, conviene subrayarlo, siempre es preciso que se diera el caso en la forma de *delincuencia organizada* que se ha referido.

Por otro lado, tenemos la figura del *agente provocador* que hace uso de la provocación para que se cometa un delito con el único objetivo de verificar que efectivamente se está cometiendo, figura que, por ahora, es

[65] Desde 1993, en Estados Unidos se han abortado 83 atentados islamistas, según ha calculado Martha Crenshaw, experta en terrorismo de *Standford University*, llegando hasta 79 la cifra de atentados abortados gracias a la acción de los *agentes provocadores* del FBI ("El enemigo está entre nosotros", *La Vanguardia*, domingo 2 de junio, p. 3).

ilegal en España, y que podría constituir una forma delictiva en sí misma por la que el agente podría ser condenado como inductor o por un acto preparatoriode proposición o provocación para cometer un delito en particular.

Finalmente, tenemos la figura del agente policial que utiliza Internet con la sola finalidad de comprobar la existencia de delitos, sin poder llegar en ningún caso a provocarlos. Esta es la única figura que hoy en día se puede utilizar en España, a pesar de que se han llegado a tramitar, sin éxito, distintas propuestas desde la Cámara del Senado al Gobierno para modificar la Ley de Enjuiciamiento Criminal y el Código Penal, con la finalidad de crear nuevas figuras (legales) para luchar contra la explotación sexual de los menores.

En el marco de la actuación policial en el ciberespacio, debe apuntarse aquí que se alzan cuestiones novedosas sobre los límites legales relativos a la posibilidad de utilizar *Facebook* y otras redes sociales como medio para investigar, prospectiva o retrospectivamente, actividades delictivas[66].

3) Desde el punto de vista del conjunto de medidas tendentes a *Eliminar las excusas*, una mención significativa merecería la adopción *efectiva* de políticas de uso de las TIC en las empresas y organizaciones públicas y privadas.

A este respecto, en otro lugar he analizado cómo prevenir conductas abusivas y delitos tecnológicos en la empresa[67]. Mediante un estudio interdisciplinar sobre políticas de uso de las TIC, prevención y gestión de "conflictos" en una muestra de empresas españolas, pudimos verificar que muchas empresas, pese a haber diseñado y comunicado una política de uso de las TIC, no habían implementado de forma operativa las políticas aprobadas o no realizaban un análisis profundo de los riesgos asociados al uso de las nuevas tecnologías. Junto al cuestionario dirigido a los responsables directivos de las empresas, se confeccionó una segunda encuesta-simulacro dirigida a los responsables de servicios informáticos,

[66] Nieto Martín, A. y Maroto Calatayud, M. (2013). Las redes sociales en Internet como instrumento de control penal: tendencias y límites. En A. Rallo Lombarte y R. Martínez Martínez (eds.), *Derecho y redes sociales* (2ª ed.). Pamplona: Civitas, pp. 430.

[67] Agustina, J.R. (2013). ¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa? Estudio interdisciplinar sobre políticas de uso de las TIC, prevención y gestión de "conflictos" en una muestra de empresas españolas. IDP. *Revista de Internet, Derecho y Política*, núm. 16, pp. 7-26.

cuyos resultados revelaron unas carencias significativas en la capacidad técnica para detectar e identificar al infractor.

En este sentido, no basta con aprobar y comunicar una política de uso y control de las TIC: es esencial el modo de implementarla, dotando de instrumentos idóneos a quienes tienen la función de velar por su cumplimiento. Así, para una adecuada estrategia de prevención de ciberdelitos en la empresa no solo deben tenerse en cuenta aspectos formales y jurídicos (relativos al control de los trabajadores y a la posible afectación al derecho a la intimidad), sino sobre todo deben establecerse los oportunos instrumentos técnicos y velar por la formación de los responsables de los servicios técnicos y los protocolos de actuación por los que se implementen eficazmente la prevención, el control y la reacción ante eventuales hechos delictivos.

VII. ALGUNAS PARADOJAS: PERFIL DE LOS OFENSORES *VERSUS* VÍCTIMAS NO TAN INGENUAS

Sentado todo lo anterior, ¿qué perfiles reúnen los cibercriminales y, en su caso, se pueden identificar ciertos patrones comunes en el perfil del ofensor? A este respecto, como señala Miró Llinares[68] no puede identificarse al *hacker* con el cibercriminal, puesto que –del mismo modo a lo que sucede en el espacio físico– nos enfrentamos a una multiplicidad de tipologías delictivas, motivaciones y, por tanto, perfiles criminológicos de diversa naturaleza. Por este motivo, siguiendo a este autor, debe distinguirse entre cibercriminalidad económica, social y política.

Asimismo, este terreno, el del perfil de los ofensores, se presta a imágenes distorsionadas de la realidad, estereotipos que conviene desmitificar. La investigación criminológica debe proporcionarnos, en este sentido, una imagen fiel con base en datos empíricos, datos que pueden dar como resultado algunas paradojas. Un ejemplo de ello es el perfil de ofensores sexuales *online* que nos proveen Wolak et al. en su estudio[69]:

[68] Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons. P.229.

[69] Wolak, J., Finkelhor, D., y Mitchell, K.J. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, 35, 424.e11– 424.e20.

Otro ejemplo en el que la construcción de un mito, en este caso claramente por parte de los medios de comunicación, parece alejarnos de la realidad es el de los terroristas aparentemente sin conexión con estructura organizada alguna, denominados por los *mass media* "lobos solitarios". En efecto, del estudio de los mecanismos que conducen a situaciones como las recientes acciones terroristas en Toulouse, Boston o Londres, los

(1) no son pedófilos (el 99% de la muestra analizada interactuaron con víctimas de entre 13–17 años); (2) aunque utilizan algunas formas de manipulación, no engañan u ocultan sus intenciones a sus víctimas, siendo éstas personas adultas interesadas en tener relaciones sexuales (las víctimas sabían acerca de las intenciones de sus ofensores antes del primer encuentro *offline*); (3) la mayoría no emplea fuerza o coacción para perpetrar el abuso sexual, ni retiene o secuestran a las víctimas (que actúan con consentimiento, incluso en múltiples ocasiones); y, finalmente, (4) resulta engañoso caracterizar a los ofensores como "extraños" a la víctima: en la mayoría de casos se habían comunicado de forma extensa antes del primer encuentro.

Lo acabado de referir tiene importantes implicaciones para las estrategias de prevención y plantea importantes cuestiones sobre el perfil de las víctimas, cuando menos en este tipo de delitos al que acabamos de hacer mención. Anteriormentehe hecho alusión a los déficits que presentan las víctimas de este particular grupo de riesgo. Por todo ello, se podría llegar a afirmar que, en realidad, no estamos (solo) ante *depredadores sexuales* en busca de víctimas ingenuamente engañadas. Por el contrario, y para ser más exactos, los abusos sexuales solo tienen lugar *si la víctima quiere*; es decir, parece que, en efecto, más tarde o más temprano la víctima "acepta". En términos coloquiales se podría decir que *se junta el hambre con las ganas de comer*, si bien en unas circunstancias que generan una cierta *simbiosis psicopatológica*. Con todo, a efectos de valorar la dimensión del problema es difícil saber el número de solicitudes, acercamientos, tretas fallidas o intentos rechazados que tienen lugar en Internet, por lo que la cifra negra–en buena parte debido a la pobreza de las encuestas de "victimización" realizadas y a la falta de conciencia de la propia victimización– dificulta enormemente por el momento un acercamiento a la realidad del problema.

En cualquier caso, si, como parece, algunas víctimas "quieren", ya se ve que no serán eficaces determinados eslóganes como "no aceptes mensajes de extraños". Ello plantea interrogantes acerca de cómo podrían

---

especialistas en la lucha antiterrorista concluyen que la expresión "solitario" no refleja correctamente la realidad. Ante la ausencia de vínculos externos, Internet se muestra como un elemento decisivo, como herramienta en la que, a través de la muy eficaz red propagandística del *yihadismo*, ese *lobo* halla una respuesta para su razón de ser y, lo que es más importante, por fin no se siente sola. ("Lobos puede; solitarios, no tanto", E. Martín de Pozuelo, *La Vanguardia*,24 de mayo de 2013, p. 4). Véase también, al respecto, Cano Paños, M.A. (2013). El caso «Mohammed Merah» en el contexto actual del terrorismo islamista. *Revista Electrónica de Ciencia Penal y Criminología* RECPC 15-02 (2013).

prevenirse este tipo de victimización, pareciendo necesario un mayor entendimientode los porqués de ese consentimiento, cesión o búsqueda activa (a pesar de posibles vicios en la voluntad) de las víctimas.

Pero, en realidad, ni las víctimas son tan ingenuas, ni su determinación es incondicional, ni los ofensores son tan sumamente sinceros: *la ocasión importa*. Es decir, la puesta en escena, la manipulación sigue existiendo y va a ser útil, por tanto, conocer los distintos tipos de *modus operandi*. En definitiva, no basta con centrarse en corregir esa *actitud enfermiza* de esos adolescentes: los entornos son relevantes.

VIII. REFLEXIONES FINALES

Concluimos con unas reflexiones sobre lo tratado, divididas en una doble perspectiva de análisis: la *perspectiva de las estrategias de prevención* (fundadas en el análisis victimológico realizado) y la *perspectiva antropológica* (relativa a los cambios introducidos por la era digital en la naturaleza humana).

Se han analizado distintos aspectos relevantes relativos a la cibervictimización desde el punto de vista criminológico/victimológico, con vistas a mejorar la protección de las víctimas desde la *perspectiva de las estrategias de prevención* (análisis *ex ante*). Utilizando la antes referida metáfora utilizada por Katyal, *Internet sigue siendo un lugar oscuro* en el que convendría arrojar algo más de luz y poner cierto orden. En el mundo físico, el deseo sentido de que las calles y barrios de nuestras ciudades sean un lugar seguro se ha traducido en todo un conjunto de medidas: desde el diseño arquitectónico del espacio público, el patrullaje policial o la creación de lazos comunitarios entre el vecindario, hasta las propias cautelas de los viandantes, que saben por qué lugares (y a qué horas) es mejor no transitar. *Mutatis mutandis*, el ciberespacio es un espacio de tránsito y sigue, en lo esencial, reglas similares, pese a que en él concurren mayores condiciones de anonimato y en él se multiplica el contacto con extraños. En ese sentido, transitar por el ciberespacio sin las debidas cautelas sería, en cierto modo, como caminar por una calle muy concurrida expuesto a todo el mundo: ya sea desnudo o ligero de ropa, o portando de forma visible joyas de preciado valor. La falta de conciencia de quienes emplean las TIC incrementa lógicamente los riesgos de victimización. Así, nuestra conducta descuidada puede reclamar de forma inadvertida la atención de innumerable observadores invisibles o parapetados en su anonimato que buscan un objetivo atractivo. Y esa ingenuidad a la que hemos aludido –*cada minuto nace un idiota nuevo*, en palabras de Barnum– nos

debería hacer *reflexionar* y frenar la forma desinhibida o *irreflexiva* en el discurrir de nuestras actividades cotidianas en el ciberespacio, de forma que asimilemos la máxima de *no hacer en el mundo virtual lo que no haría en el mundo real*. Aquí se abren muchos campos a la investigación. Entre muchos, uno me parece especialmente relevante: qué correlaciones se pueden identificar entre el contexto personal, social y virtual con las actitudes desinhibidoras de los individuos en sus actividades cotidianas y no cotidianas.

En cuanto a la *perspectiva antropológica*, la era digital ha supuesto, como hemos visto, cambios de una enorme trascendencia no solo en la vida cotidiana de las personas sino en su mismo modo de ser y de pensar. Ante este hecho sociológico, he tratado de anclar los cambios sufridos en la naturaleza del ser humano y en su vulnerabilidad innata al contexto que le circunda. En la Antigua Grecia, la célebre disputa filosófica entre Heráclito y Parménides sobre la tesis del *flujo universal de los seres* –«panta rei» (*πάντα ρεῖ*): todo fluye–, ya puso de manifiesto que, en realidad, aunque *un hombre no puede bañarse dos veces en el mismo río* (pues la segunda vez, el río ya no es el mismo, como tampoco lo es el hombre), no por ello el ser humano pierde sus atributos esenciales a pesar del fluir de los cambios. En efecto, en la naturaleza humana hay una parte esencial que resiste a los cambios históricos y culturales, y también tecnológicos, pese a que tales cambios pueden, como hemos visto, afectar enormemente las condiciones relacionales, los estilos de vida y, en lo que aquí interesaba, las oportunidades de victimización. El diagnóstico que hemos apuntado se podría sintetizar en que las tendencias desfragmentadoras en la unidad de vida de las personas, fruto de la era digital, elevan considerablemente los riesgos de victimización. Por ello, sin dejar de considerar los avances positivos que ha supuesto la era digital y la generalización del uso de las TIC e Internet, se debería iniciar la senda *en búsqueda de la identidad perdida* para lograr evitar la desfragmentación del yo. He aquí un reto de enorme calado antropológico que tenemos por delante en la formación de esas nuevas generaciones de nativos digitales.